

Instale y configure el OpenAM Identity Provider (IdP) para Cisco Identity Service (IdS) para habilitar el SSO

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Instalar](#)

[Requisitos del sistema](#)

[Sistemas operativos](#)

[Entorno Java](#)

[Requisitos del contenedor de aplicaciones web](#)

[Navegadores admitidos](#)

[Requisitos del almacén de datos](#)

[Requisitos mínimos de hardware](#)

[Instalar](#)

[Obtenga el software OpenAM](#)

[Requisitos previos](#)

[Instalación de la aplicación web OpenAM](#)

[Ejecutar el servicio OpenAM](#)

[Configurar](#)

[Configurador OpenAM](#)

[Configurar OpenAM como IdP](#)

[Configuración del círculo de confianza](#)

[Crear proveedor de identidad alojado](#)

[Configurar clave de firma](#)

[Importar entidad de proveedor de servicios](#)

[Firma de solicitud/respuesta](#)

[Asignación de atributos](#)

[Editar círculo de confianza](#)

[Descargar metadatos de OpenAM IdP](#)

[Configuración adicional para SSO:](#)

Introducción

Este documento describe la configuración en OpenAM Identity Provider (IdP) para habilitar el inicio de sesión único (SSO).

Modelos de implementación de Cisco IdS

Producto	Implementación
UCCX	Copresidente
PCCE	Coresidente con CUIIC (Cisco Unified Intelligence Center) y LD (Live Data)
UCCE	Coresidente con CUIIC y LD para implementaciones 2k. Independiente para implementaciones de 4000 y 12 000.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Unified Contact Center Express (UCCX) versión 11.6 o Cisco Unified Contact Center Enterprise versión 11.6 o Packaged Contact Center Enterprise (PCCE) versión 11.6, según corresponda.

Nota: Este documento hace referencia a la configuración con respecto a Cisco Identity Service (IdS) y el Identity Provider (IdP). El documento hace referencia a UCCX en las capturas de pantalla y los ejemplos; sin embargo, la configuración es similar con respecto al servicio de identificación de Cisco (UCCX/UCCE/PCCE) y al idP.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Instalar

Nota: Este documento hace referencia a la versión 10.0.1 de OpenAM como parte de la calificación con SSO

Requisitos del sistema

Sistemas operativos	Entorno Java	Requisitos del contenedor de aplicaciones web	Navegadores admitidos	Requisitos del almacén de datos	Requisitos mínimos de hardware
<ul style="list-style-type: none"> • Microsoft Windows Server 2003, 2008 R2 • Linux 2.6 y 3.0 • Oracle Solaris 10 	<p>La versión 10.0.1 de OpenAM requiere Java Development Kit 1.6, al menos 1.6.0_10. ForgeRock recomienda que utilice al menos la versión 1.6.0_27 debido a las correcciones de seguridad. ForgeRock ha probado esta versión de OpenAM principalmente con Oracle Java SE JDK. OpenAM Java SDK soporta Java Development Kit 1.5 o 1.6.</p>	<ul style="list-style-type: none"> • Apache Tomcat 6.0.x, 7.0.x • GlassFish v2 • JBoss Enterprise Application Platform 4.x y 5.x • Servidor de aplicaciones JBoss 7.x • Embarcadero 7 • Oracle WebLogic Server 11g • Oracle WebLogic Server 12c <p>Si se ejecuta como usuario no raíz, el contenedor de aplicaciones web debe poder escribir en su propio directorio principal, donde OpenAM almacena los archivos de configuración.</p>	<ul style="list-style-type: none"> • Cromo y cromos 16 y posteriores • Firefox 3.6 y versiones posteriores • Internet Explorer (versión 7 y posteriores) • Safari 5 y posteriores 	<ul style="list-style-type: none"> • OpenDJ de ForgeRock • Microsoft Active Directory • Servidor de directorio IBM Tivoli • OpenDS • Oracle Directory Server Enterprise Edition 	<ul style="list-style-type: none"> • 1 GB de RAM libre para OpenAM <p>Puede implementarse OpenAM en cualquier hardware compatible con la combinación de software necesaria.</p>

Instalar

Obtenga el software OpenAM

- Descargue las versiones de OpenAM 10.0.1 desde <https://backstage.forgerock.com/downloads/OpenAM/OpenAM%20Enterprise/10.0.1/OpenAM%201>
- Para cada versión de los servicios centrales de OpenAM, puede descargar el paquete completo como un archivo .zip, sólo el archivo .war de OpenAM, sólo las herramientas administrativas como un archivo .zip
- Después de descomprimir el archivo de todo el paquete, se obtiene un directorio opensso con un archivo README, un conjunto de archivos de licencia y los directorios

Requisitos previos

Asegúrese de que dispone del software necesario para los servicios principales de OpenAM antes de la instalación.

- Un entorno de tiempo de ejecución de Java 6
- Instalar Apache Tomcat como contenedor de aplicaciones web
- Los servicios de núcleo de OpenAM requieren un tamaño mínimo de pila de memoria virtual de Java (JVM) de 1 GB y un tamaño de generación permanente de 256 MB. Aplique las opciones de JVM cuando defina JAVA_OPTS en el archivo catalina antes del inicio del servidor de aplicaciones tomcat - `-Xmx1024m -XX:MaxPermSize=256m`

Por ejemplo, set `JAVA_OPTS=%JAVA_OPTS% -Xmx1024m -XX:MaxPermSize=256m -Xms512m`

- Instale Microsoft Active Directory como almacén de datos con pocos usuarios.

Instalación de la aplicación web OpenAM

El archivo `deployable-war/opensso.war` contiene todos los componentes y ejemplos del servidor OpenAM bajo el directorio `opensso`.

Implementación de OpenAM en el contenedor Tomcat

Copie el archivo `opensso.war` en el directorio donde se almacenan las aplicaciones web de tomcat. Cambie el nombre del archivo `opensso.war` por `openam.war`. Reinicie el servicio tomcat.

Verifique la pantalla de configuración inicial en su navegador en <http://<FQHN>:8080/openam>



Configuration Options

Please select a configuration option.

Default Configuration

Enter only the passwords for the default administrator and the agent accessor. All other data is configured using default parameters. This option should be used primarily for evaluation or development purposes.

[Create Default Configuration](#)

Custom Configuration

Allows you to specify all configuration parameters including the type of data store, encryption properties, user data store, etc. This option has the most flexibility in setting up your installation.

[Create New Configuration](#)

Copyright © 2010-2011 ForgeRock AS, Philip Pedersens vel 1, 1366 Lysaker, Norway. All rights reserved. Licensed for use under the Common Development and Distribution License (CDDL), see <http://www.forgerock.com/license/CDDLv1.0.html> for details. This software is based on the OpenSSO/OpenAM open source project and the source includes the copyright works of other authors, granted for use under the CDDL. This distribution may include other materials developed by third parties. All Copyrights and Trademarks are property of their owners.

Ejecutar el servicio OpenAM

Openam es una sencilla aplicación web alojada en un servidor tomcat. Por lo tanto, simplemente inicie su servidor tomcat y por lo tanto sea capaz de acceder al servicio web OpenAM.

Configurar

Configurador OpenAM

El proceso de configuración personalizada de OpenAM permite establecer fácilmente muchas opciones de configuración comunes, por lo que con un mayor esfuerzo antes de la configuración, se guardan los pasos de configuración requeridos más adelante.

Configuración general

Haga clic en la opción [Create New Configuration](#) y elija la contraseña para la cuenta de administrador predeterminada (amAdmin). La contraseña debe tener al menos 8 caracteres.

OpenAM Configurator

Custom Configuration Option

- General
- 2. Server Settings
- 3. Configuration Store
- 4. User Store
- 5. Site Configuration
- 6. Agent Information
- 7. Summary

Step 1: General

Enter the password for the default user, amAdmin. The password must be at least 8 characters in length. If this configuration will be part of an existing deployment, the password you enter must match that of the original deployment.

* Indicates required field

Default User Password

Default User [amAdmin]

* Password OK

* Confirm Password

Previous Next Cancel

Una vez que se haya introducido una contraseña válida dos veces, aparecerá el botón next (siguiente) y la configuración podrá continuar.

Configuración del servidor


De forma predeterminada, la dirección URL del servidor es el nombre de dominio completo del servidor.

Nota: Es importante que el usuario que ejecuta Apache Tomcat tenga acceso de escritura al directorio Configuration. Como resultado ~/openam/config es apropiado para este propósito. Las configuraciones regionales de plataforma compatibles son en_US (inglés), de (alemán), es (español), fr (francés), ja (japonés), zh_CN (chino simplificado) o zh_TW (chino tradicional).

OpenAM Configurator ✕

Custom Configuration Option

- 1. General
- ➔ **Server Settings**
- 3. Configuration Store
- 4. User Store
- 5. Site Configuration
- 6. Agent Information
- 7. Summary

Step 2: Server Settings 

Confirm the following settings to use for the server.

* Indicates required field

Server Settings

* Server URL	<input type="text" value="http://openamserver.cisco.com:8080"/>
* Cookie Domain	<input type="text" value=".cisco.com"/>
* Platform Locale	<input type="text" value="en_US"/>
* Configuration Directory	<input type="text" value="C:/Users/Administrator/openam"/>

Previous Next Cancel

Configuración de almacén de datos

Para la configuración de un único servidor, no es necesario cambiar estos parámetros.

OpenAM Configurator

Custom Configuration Option

- 1. General
- 2. Server Settings
- **Configuration Store**
- 4. User Store
- 5. Site Configuration
- 6. Agent Information
- 7. Summary

Step 3: Configuration Data Store Settings

If no other OpenAM instance already exists in the environment, then choose First Instance. If one or more OpenAM instances already exist in the environment, choose Add to Existing Deployment.

First Instance Add to Existing Deployment? * Indicates required field

Configuration Store Details

Configuration Data Store OpenAM OpenDJ or Sun Java System Directory Server

* SSL/TLS Enabled

* Host Name

* Port

* Admin Port

* JMX Port

* Encryption Key

* Root Suffix

Configuración del almacén de datos de usuario

La configuración del almacén de datos de usuario conecta OpenAM al almacén de datos de Microsoft Active Directory.

OpenAM Configurator X

Custom Configuration Option

1. General
2. Server Settings
3. Configuration Store
- ➔ 4. User Store
5. Site Configuration
6. Agent Information
7. Summary

Step 4: User Data Store Settings ?

You can use the data store that comes with the OpenAM configuration data store, or you can use a different user data store. A good practice for setting up production environments is to use an external user data store, one that is different than the OpenAM user data store. Please note that Policy Service and LDAP Authentication Module shall be configured to use the Directory Administrator DN and Password provided here.

OpenAM User Data Store
 Other User Data Store

* Indicates required field

User Store Details

* User Data Store Type

Sun Java System Directory Server
 Active Directory with Host and Port
 Active Directory Application Mode

OpenDJ
 AD with Domain Name
 IBM Tivoli Directory Server

* SSL/TLS Enabled

* Directory Name

* Port

* Root Suffix

* Login ID

* Password OK

Previous
Next
Cancel

- Tipo de almacén de datos de usuario: Active Directory con host y puerto
- SSL/TLS habilitado: No aplicable
- Nombre del directorio: <Domain Name of AD Server>
- Puerto: 389
- Sufijo raíz: dc=cisco,dc=com
- ID de conexión: cn=<nombre de usuario de AD>,cn=users,dc=cisco,dc=com
- Contraseña <Contraseña de usuario de AD>

Nota: El configurador no proporciona una opción para continuar hasta que se hayan especificado correctamente todas las opciones y se haya conectado correctamente a la instancia de Active Directory.

Configuración del sitio

En la pantalla Configuración del sitio, puede configurar OpenAM como parte de un sitio en el que la carga esté equilibrada entre varios servidores OpenAM. Para la primera instalación de OpenAM, acepte los valores predeterminados.

OpenAM Configurator

Custom Configuration Option

- 1. General
- 2. Server Settings
- 3. Configuration Store
- 4. User Store
- **Site Configuration**
- 6. Agent Information
- 7. Summary

Step 5: Site Configuration

Will this instance be deployed behind a load balancer as part of a site configuration?

No
 Yes

* Indicates required field

Site Configuration Details

This is the first instance of OpenAM, and no site configurations currently exist. To create a new site configuration, provide the following information

* Site Name

* Load Balancer URL

Información del agente

En la pantalla Agent Information (Información de agente), proporcione una contraseña de al menos 8 caracteres que los agentes de políticas utilizarán para conectarse a OpenAM.

OpenAM Configurator ✕

Custom Configuration Option

- 1. General
- 2. Server Settings
- 3. Configuration Store
- 4. User Store
- 5. Site Configuration
- ➔ **Agent Information**
- 7. Summary

Step 6: Default Policy Agent User

These settings are used by OpenAM policy agents for retrieving policy agent properties.

* Indicates required field

Policy Agent User

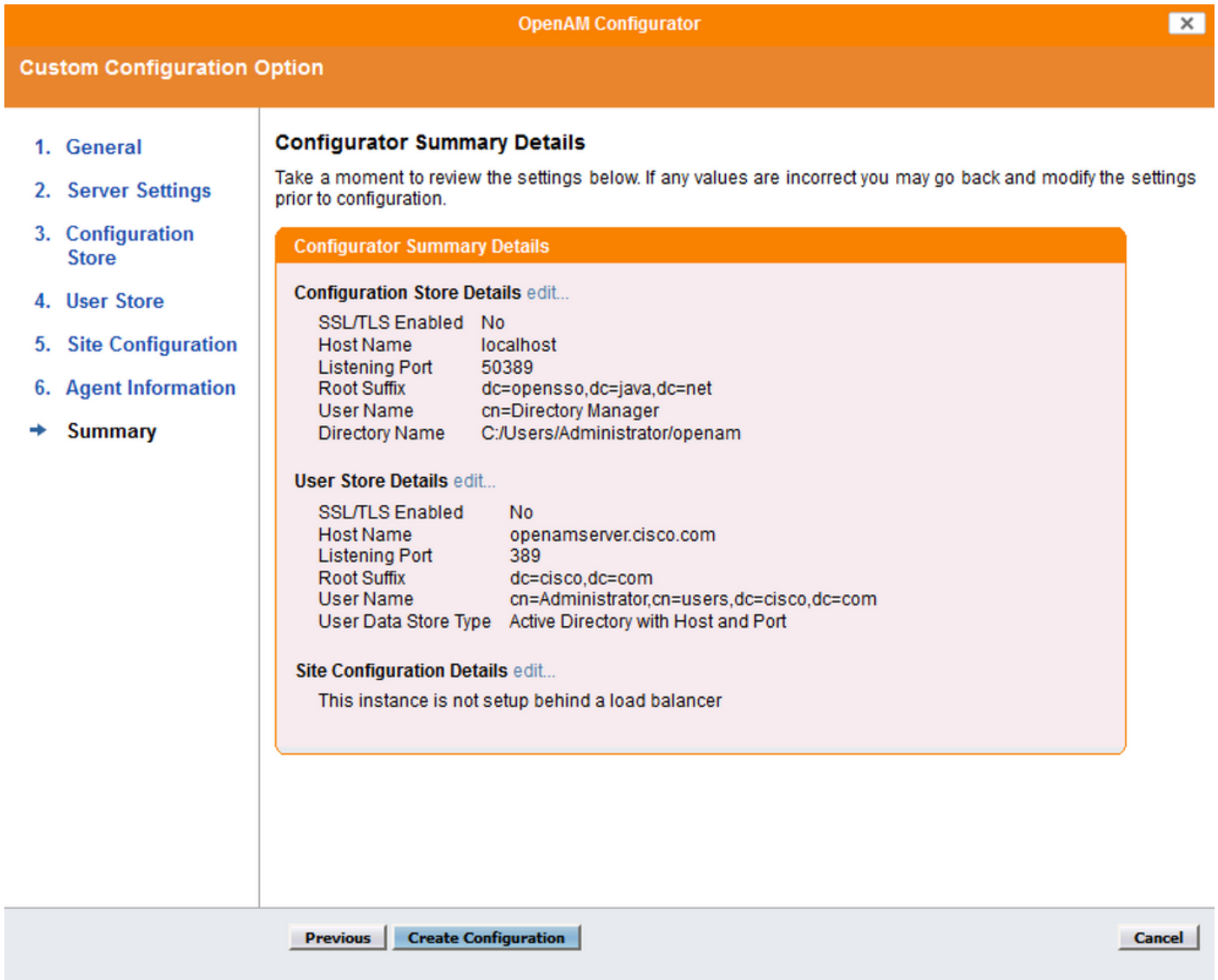
Default Policy Agent [UriAccessAgent]

* Password OK

* Confirm Password

Summary

Revise la información y haga clic en Create Configuration .



Progreso de configuración

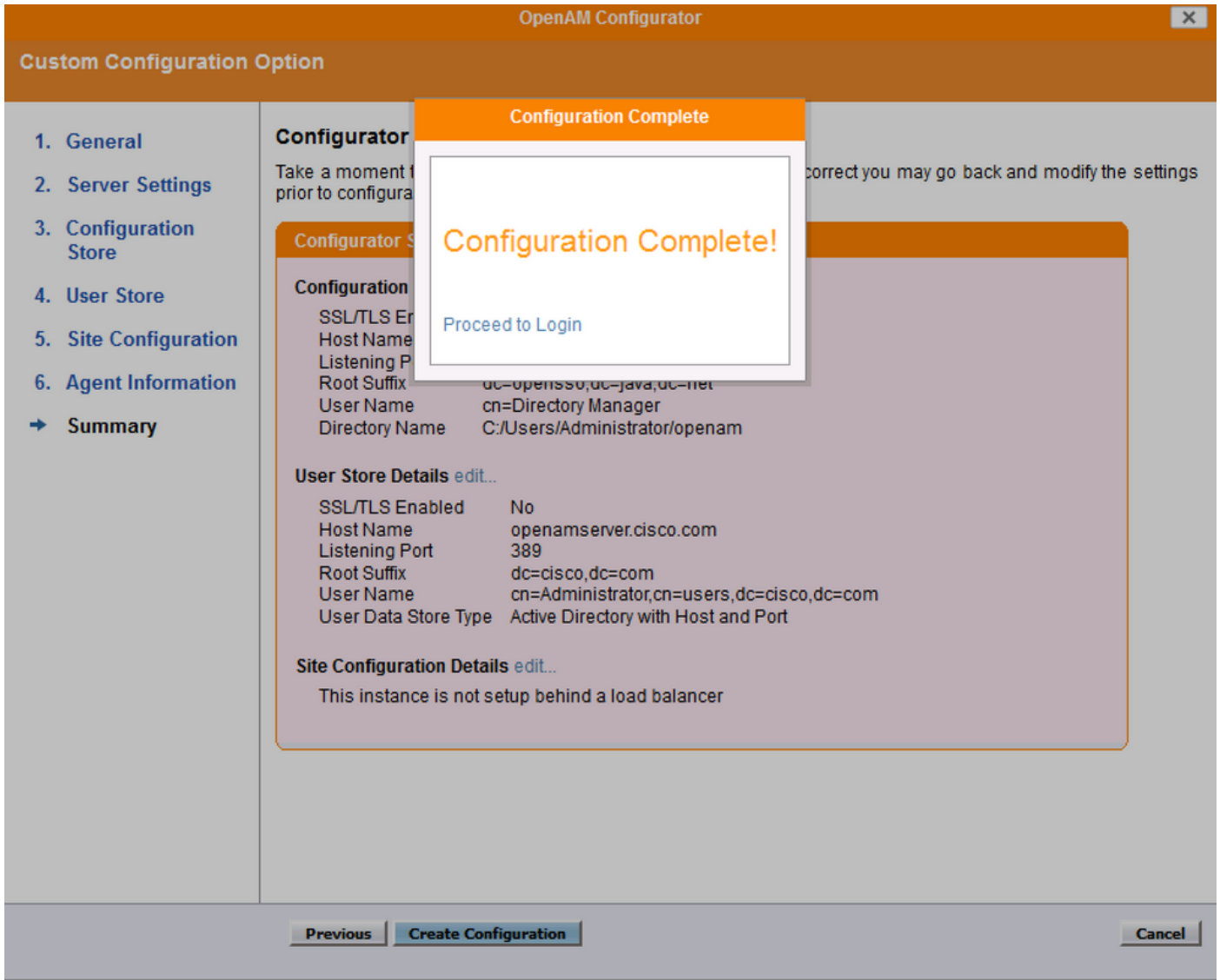
La pantalla Progreso de la configuración muestra el progreso de la instalación. Todos los resultados de esta pantalla y los errores se escriben en el archivo: `~/openam/config/install.log`.

Please wait... configuration in progress...



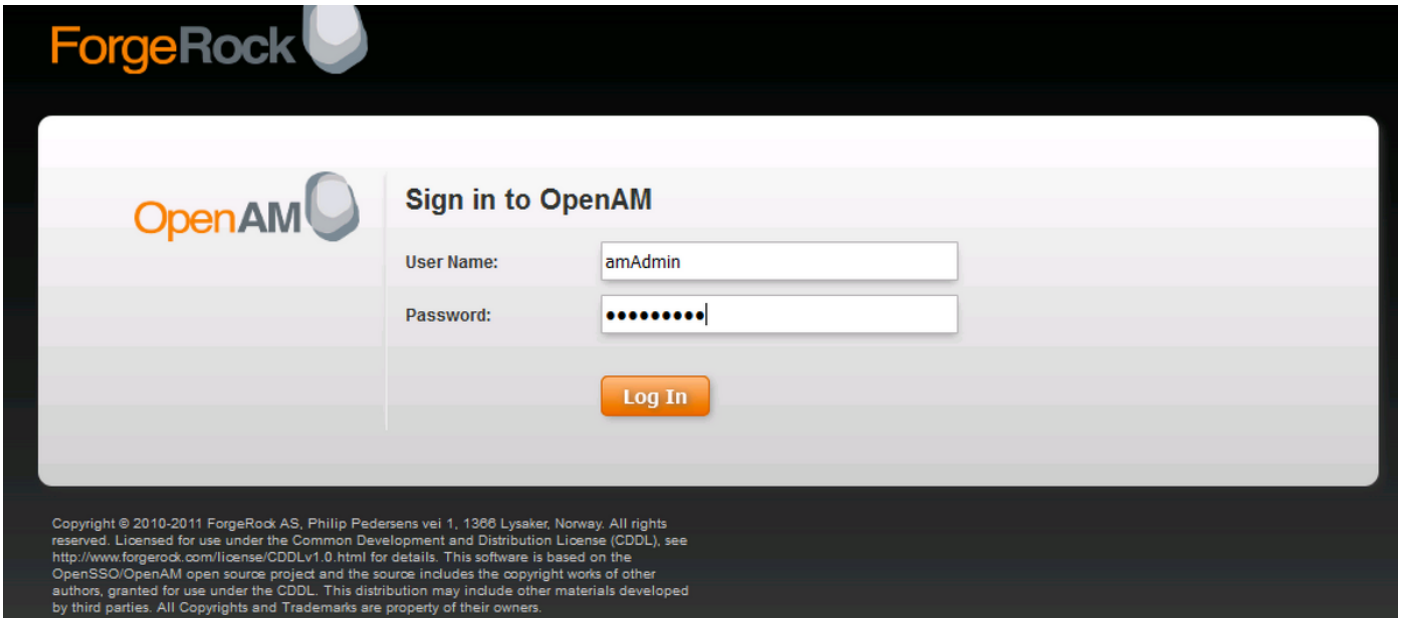
```
Checking configuration directory C:/Users/Administrator/openam....Success.  
Installing OpenAM configuration store...Success RSA/ECB/OAEPWithSHA1AndMGF1Padding.  
Extracting OpenDJ, please wait...Complete  
Running OpenDJ setupSetup command: --cli --adminConnectorPort 4444 --baseDN  
dc=openasso,dc=java,dc=net --rootUserDN cn=Directory Manager --ldapPort 50389 --skipPortCheck  
--rootUserPassword xxxxxx --jmxPort 1689 --no-prompt --configFile C:/Users/Administrator/openam  
/opens/config/config.ldif --doNotStart --hostname openamserver.cisco.com OpenDJ 2.4.5  
Please wait while the setup program initializes...
```

Configuración finalizada



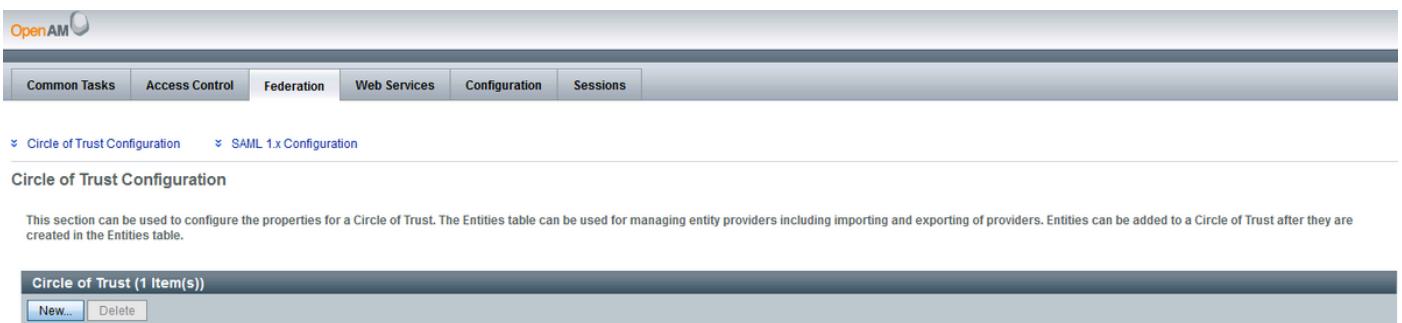
Configurar OpenAM como IdP

- Haga clic en Proceed to Login o Access through URL <http://<FQDN of OpenAM>:8080/openam>, y luego inicie sesión como administrador de OpenAM
- Cuando accede a OpenSSO Enterprise por primera vez, se le dirige al Configurator para realizar la configuración inicial de OpenSSO Enterprise
- Seleccionar configuración predeterminada
- Es necesario configurar las contraseñas para OpenAMserver
- Configure las contraseñas e inicie sesión en la interfaz del servidor OpenAM

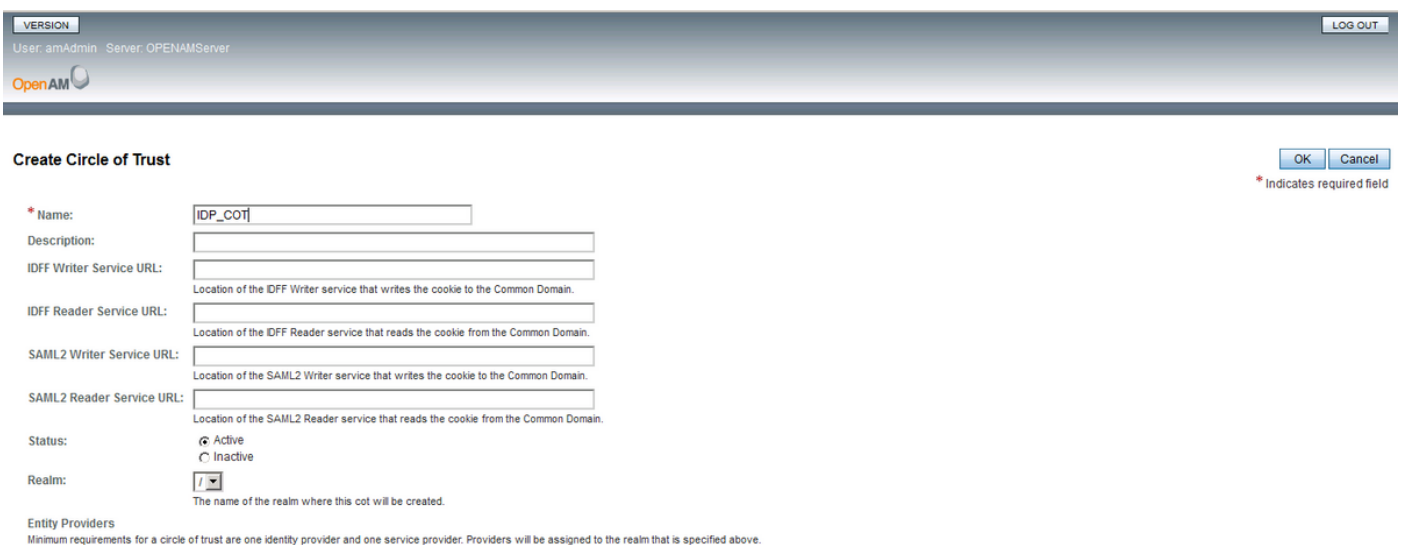


Configuración del círculo de confianza

Navegue hasta la pestaña de federación y haga clic en el botón Nuevo en la sección Círculo de confianza



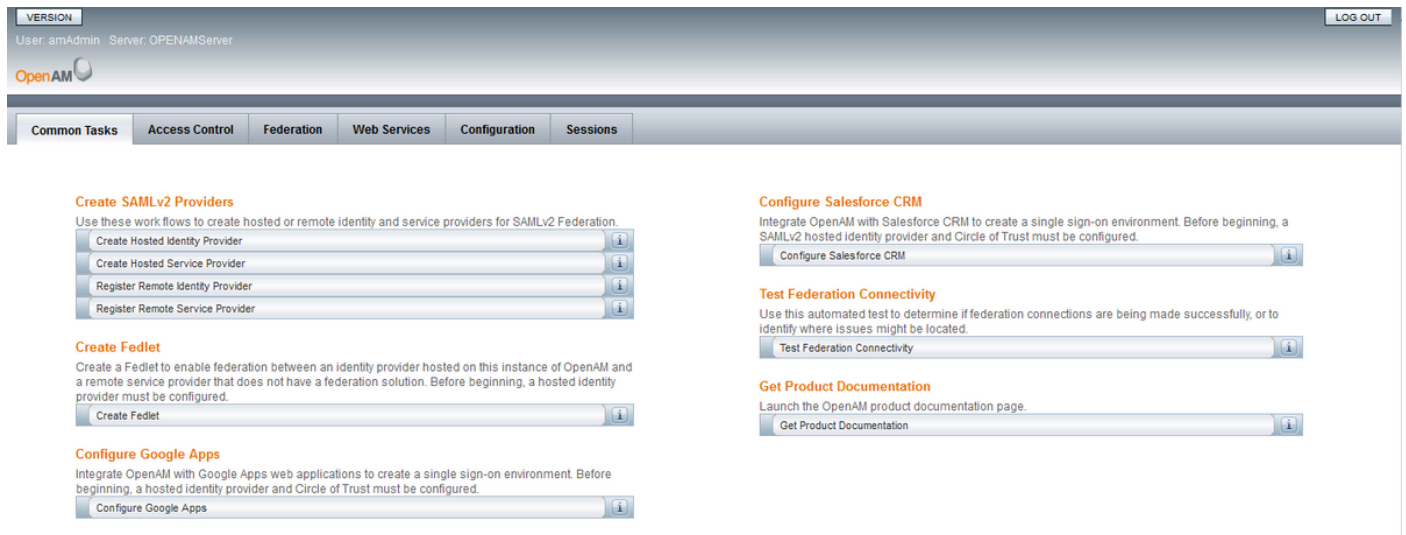
Cree un círculo de confianza con un nombre único para el círculo de confianza IdP y haga clic en Aceptar



Nota: El proveedor de servicios y el idP deben estar en el mismo círculo de confianza (CoT) para que funcione el SSO de SAML.

Crear proveedor de identidad alojado

Vaya a la pestaña Tareas comunes y haga clic en Crear proveedor de identidad alojado y crear un IdP alojado (deje los valores predeterminados configurados y guarde los parámetros).



The screenshot shows the OpenAM administration interface. At the top, there is a header with 'VERSION', 'User: amAdmin', 'Server: OPENAMServer', and a 'LOG OUT' button. Below the header is a navigation menu with tabs for 'Common Tasks', 'Access Control', 'Federation', 'Web Services', 'Configuration', and 'Sessions'. The main content area is divided into several sections:

- Create SAMLv2 Providers:** Includes instructions and buttons for 'Create Hosted Identity Provider', 'Create Hosted Service Provider', 'Register Remote Identity Provider', and 'Register Remote Service Provider'.
- Create Fedlet:** Includes instructions and a 'Create Fedlet' button.
- Configure Google Apps:** Includes instructions and a 'Configure Google Apps' button.
- Configure Salesforce CRM:** Includes instructions and a 'Configure Salesforce CRM' button.
- Test Federation Connectivity:** Includes instructions and a 'Test Federation Connectivity' button.
- Get Product Documentation:** Includes instructions and a 'Get Product Documentation' button.

Se muestra el círculo de confianza creado anteriormente



The screenshot shows the 'Circle of Trust' configuration page. It includes the following elements:

- Circle of Trust:** A heading for the configuration section.
- Choose from existing circles of trust listed or provide one to be created in which to include this IDP. A CoT is a group of IDPs and SPs that trust each other and provides the confines within which all SAMLv2 communications are performed.**
- Circles of Trust:** Radio buttons for 'Add to existing' and 'Add to new'.
- * Existing Circle of Trust:** A dropdown menu with 'IDP_COT' selected.

Configurar clave de firma

Navegue hasta la pestaña Federation y haga clic en el proveedor de identidad alojado agregado en la sección Proveedores de entidad. Navegue hasta la sección Contenido de la aserción y configure el valor del campo Firma como prueba en la sección Alias de certificado. Este es el certificado que se utilizaría para firmar la afirmación SAML.

- ✖ Signing and Encryption
- ✖ Assertion Time
- ✖ Bootstrapping
- ✖ NameID Format
- ✖ Basic Authentication
- ✖ Authentication Context
- ✖ Assertion Cache

Signing and Encryption

Request/Response Signing

Select the checkbox for each request/response that should be signed

- Authentication Request:
- Artifact Resolve:
- Logout Request:
- Logout Response :
- Manage Name ID Request:
- Manage Name ID Response:

Encryption

NameID Encryption:

Certificate Aliases

Signing:

The alias (name) of the certificate to be used to sign assertions.

Importar entidad de proveedor de servicios

Navegue hasta la pestaña Federation y haga clic en el botón Import Entity... en la sección Entity Providers.

The screenshot shows the OpenAM web interface. The top navigation bar includes 'Common Tasks', 'Access Control', 'Federation', 'Web Services', 'Configuration', and 'Sessions'. The 'Federation' tab is active, and the 'SAML 1.x Configuration' sub-tab is selected. The main content area is titled 'Circle of Trust Configuration' and contains a table with one item, 'IDP_COT'. Below this is the 'Entity Providers (3 Item(s))' section, which includes a table and an 'Import Entity...' button.

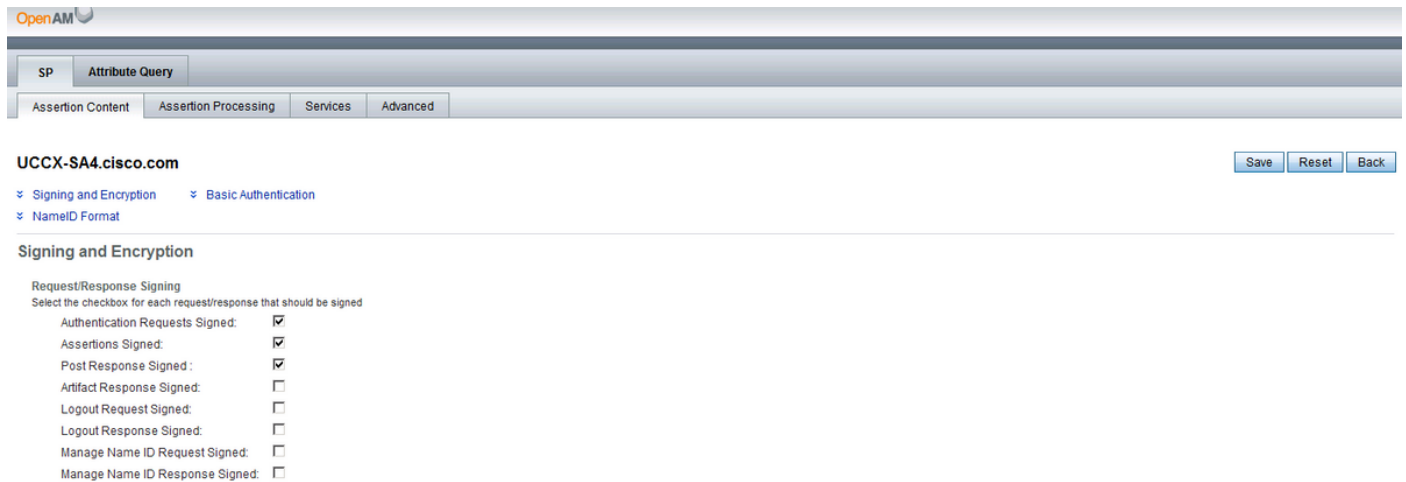
Name	Entities	Realm	Status
IDP_COT	UCCX-HA-Node1.cisco.com saml2 https://openamserver.cisco.com:8443/openam saml2 UCCX-SA4.cisco.com saml2	/	Active

Cargue el archivo de entidad del proveedor de servicios (sp.xml) y guarde la página.

The screenshot shows the 'Import Entity Provider' form. It includes a description of the page's purpose and a list of required fields: 'Realm Name', 'Where does the metadata file reside?' (with radio buttons for URL and File), 'URL where metadata is located' (with an 'Upload...' button), 'Where does the extended data file reside?' (with radio buttons for URL and File), and 'URL where extended data is located' (with a text input field). There are 'OK' and 'Cancel' buttons at the top right.

Firma de solicitud/respuesta

Haga clic en la entidad importada y active la firma para Solicitud/Respuesta



The screenshot shows the OpenAM configuration interface for the service provider 'UCCX-SA4.cisco.com'. The 'Attribute Query' tab is selected, and the 'Advanced' sub-tab is active. The 'Signing and Encryption' section is expanded, showing a list of signing options with checkboxes. The following table represents the state of these checkboxes:

Request/Response	Checked
Authentication Requests Signed:	<input checked="" type="checkbox"/>
Assertions Signed:	<input checked="" type="checkbox"/>
Post Response Signed:	<input checked="" type="checkbox"/>
Artifact Response Signed:	<input type="checkbox"/>
Logout Request Signed:	<input type="checkbox"/>
Logout Response Signed:	<input type="checkbox"/>
Manage Name ID Request Signed:	<input type="checkbox"/>
Manage Name ID Response Signed:	<input type="checkbox"/>

Asignación de atributos

Navegue hasta Procesamiento de aserción y agregue un atributo de asignación para uid y user_principal según la configuración de Directorio y OpenAM. Haga clic en Guardar.



The screenshot shows the OpenAM configuration interface for 'UCCX-SA4.cisco.com' in the 'Attribute Mapper' section. The 'Artifact Message Encoding' sub-tab is active. The 'Attribute Map' section shows a list of 'Current Values' with a 'Remove' button next to each. The values are:

- uid=sAMAccountName
- user_principal=userPrincipalName

Below the list is a 'New Value' input field and an 'Add' button. A note at the bottom states: 'This mapping is the configuration used by the Attribute Mapper. Mapping should be defined as SAML ATTRIBUTE NAME=PROFILE ATTRIBUTE NAME in assertion. Example: EmailAddress=mail, Address=postaladdress.'

Nota: Tanto los atributos uid como user_principal son obligatorios, ya que Service Provider (SP) identifica la identidad de un usuario autenticado con la ayuda de estos. Además, asegúrese de que los atributos sAMAccountName y userPrincipalName también estén asignados en el Editor de atributos de las propiedades de usuario de Active Directory.

Editar círculo de confianza

Desplácese hasta la ficha Federación y haga clic en Círculo de confianza agregado y asegúrese de mover el IdP (servidor OpenAm) y la entidad Proveedor de servicios de las secciones Disponible a Seleccionado en la sección Proveedores de entidades. Esto asigna al IdP y al Proveedor de Servicios que estén en el mismo Círculo de Confianza.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).